UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

SHIRA KOHN and ANDRES VIVAS, *on behalf of themselves and all others similarly situated*,	§	Lead Case No. 4:23-cv-03035
	§	Consolidated Case:
Plaintiffs,	§	4:23-cv-03643
v.	§	
LOREN D. STARK COMPANY, INC.,	§	Judge Lee H. Rosenthal
Defendant.	§	

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Shira Kohn and Andres Vivas (collectively, "Plaintiffs") bring this Class Action Complaint against Loren D. Stark Company, Inc. ("Defendant" or "LDSC"), on behalf of themselves and all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach resulting from LDSC's failure to implement reasonable and industry standard data security practices.

2. Defendant is a third-party retirement plan consulting and administration firm headquartered in Houston, Texas. Defendant's services include retirement and pension plan design and document preparation, compliance testing and reporting, annual plan participant ERISA compliance statements, and participant loan and distribution documentation.

3. Defendant collected and maintained certain personally identifiable information("PII")[1] of Plaintiffs and Class Members, who are (or were) employees at companies that contracted with LDS for services, including but not limited to Plaintiffs' and Class Members' full names and Social Security numbers.

4. To provide these services, and in the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiffs' and Class Members' PII.

5. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Plaintiffs and at least 51,659[2] other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on October 18, 2022, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive PII belonging to Plaintiffs and Class Members which was being kept unprotected (the "Data Breach").

6. Plaintiffs further seek to hold Defendant responsible for not ensuring that the PII was maintained in a manner consistent with industry standards.

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/f7119163-666d-4163-8805-08936cb9558c.shtml (last visited August 17, 2023).

7. On or about August 4, 2023, Defendant notified state Attorneys General and many Class Members about the widespread Data Breach (the "Notice Letter").[3]

8. While Defendant claims to have discovered the Data Breach as early as October 18, 2022, Defendant did not begin informing victims of the Data Breach until August 4, 2023, over nine months later. Indeed, Plaintiffs and Class Members were wholly unaware of the Data Breach until they received Notice Letters from Defendant dated August 4, 2023. During this time, Plaintiffs and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

9. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited identity monitoring services Defendant offered in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiffs' and Class Members' PII remains in the possession of criminals.

10. By acquiring, utilizing, and benefiting from Plaintiffs' and Class Members' PII for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiffs and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiffs' and Class Members'

[3] Sample Notice Letter available at the Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/f7119163-666d-4163-8805-08936cb9558c/83660066-0c76-45f6-9302-300cb7d438d2/document.html (last visited August 17, 2023).

PII in its possession and to keep Plaintiffs' and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

11. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiffs' and Class Members' PII from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiffs' and Class Members' PII.

12. Currently, the full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

13. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiffs' and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third party.

14. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and

accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

15. Based on the type of sophisticated and targeted criminal activity, the type of PII involved, and Defendant's admission that the PII was accessed, it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiffs' and Class Members' PII, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiffs' and Class Members' PII, including full names and Social Security numbers, for the purposes of utilizing or selling the PII for use in future fraud and identity theft related cases.

16. As a result of Defendant's failures and the Data Breach, Plaintiffs' and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

17. As Defendant instructed, advised, and warned in its Notice Letter discussed below, Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

18. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the

materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) deprivation of value of their PII; (h) invasions of their privacy; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

19. Plaintiffs bring this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

20. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

21. Plaintiffs seek remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

22. Plaintiff Shira Kohn is an adult individual and, at all relevant times herein, a resident and citizen of New York state.

23. Plaintiff Andres Vivas is an adult individual and, at all relevant times herein, a resident and citizen and citizen of the state of Florida.

24. Defendant Loren D. Stark Company, Inc., is a Texas corporation with its principal place of business at 10750 Rockley Road, Houston, TX 77099-3516. The registered agent for service of process is Donald D. Stark, 10750 Rockley Road, Houston, Texas 77099.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiffs Kohn and Vivas, is a citizen of a state different from Defendant.

26. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business is in this District, Defendant regularly conducts business in Texas, and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

27. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

28. Defendant LDSC is a third-party administrator of employee insurance plans headquartered in Austin, Texas. LDSC offers retirement and pension plan design and document preparation, compliance testing and reporting, annual plan participant ERISA compliance statements, participant loan and distribution documentation.

29. Plaintiffs and Class Members are current and former employees at companies that contracted with Defendant for services.

30. As a condition of their employment at Defendant's clients, Plaintiffs and Class Members were required to entrust Defendant, directly or indirectly, with highly sensitive personal information.

31. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

32. Upon information and belief, Defendant made promises and representations to its clients' employees, including Plaintiffs and Class Members, that the PII collected from them as a condition of their employment at Defendant's clients would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

33. Defendant's Privacy Policy, posted on its website, states that LDSC "values your trust and is committed to the responsible management, use, and protection of personal information.[4]

34. Plaintiffs and Class Members provided their PII, directly or indirectly, to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members

35. In the ordinary course of its business, LDSC maintains the PII of its customers' current and past employees, consumers, customers, and others including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;

[4] *Privacy Policy*, https://ldsco.net/Privacy.aspx (last visited Jan. 12, 2024).

- Social Security number;
- Financial information;
- Employment information; and
- Other information that Defendant may deem necessary to administer its retirement and financial products.

36. Additionally, LDSC may receive PII from other individuals and/or organizations including Plaintiffs' and Class Members' employers, insurance carriers, and in connection with enrollment in employee insurance and retirement benefit plans.

37. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to consumers, LDSC, upon information and belief, promises to, among other things: keep protected health information private; comply with industry standards related to data security and PII, inform consumers of its legal duties and comply with all federal and state laws protecting consumer PII; only use and release PII for reasons that relate to medical care and treatment; and, provide adequate notice to individuals if their PII is disclosed without authorization.

38. At every step, LDSC holds onto sensitive PII and has a duty to protect that PII from unauthorized access.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

40. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

41. Plaintiffs and Class Members relied on Defendant to implement and follow

adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use their PII solely for proper business services and purposes, and to prevent the unauthorized disclosure of their PII.

The Cyberattack and Data Breach

42. On or about October 18, 2022, LDSC detected unauthorized access to certain computer systems within its network environment. The unauthorized access was the result of a cybersecurity incident.[5]

43. LDSC took steps to secure its network systems and investigated the nature and scope of the incident with the consultation of third-party cybersecurity professionals.[6]

44. Through its investigation, LDSC determined that its network and servers were subject to a cyberattack that impacted its network resulting in information on its network being accessed and acquired without authorization.[7]

45. Upon information and belief, Plaintiffs' and Class Members' PI was exfiltrated and stolen in the attack.

46. Furthermore, the investigation determined that the accessed systems contained PII. Upon information and belief, this PII was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

47. The type of PII accessed by the unauthorized actor in the Data Breach includes full names and Social Security numbers.[8] The Social Security numbers were unencrypted.

---

[5] *See* Notice Letter

[6] *Id.*

[7] *Id.*

[8] *Id.*

48. While LDSC stated in the Notice Letter that the unusual activity occurred and was discovered on October 18, 2022, LDSC did not begin notifying victims until August 4, 2023, over 9 months after LDSC discovered the Data Breach occurred.[9]

49. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

50. Plaintiffs and Class Members provided their PII to directly, or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

51. Through its Notice Letter, LDSC also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.

52. LDSC has offered abbreviated, non-automatic credit monitoring services to victims thereby identifying the harm posed to Plaintiffs and Class Members as a result of the Data Breach, which does not adequately address the lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves PII that cannot be changed, such as Social Security numbers.

53. Beginning on or around August 4, 2022, Defendant issued Notice Letters to Plaintiffs and Class Members. In total, Defendant notified at least 51,659 individuals.[10]

---

[9] *Id.*

[10] See *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/f7119163-666d-4163-8805-

54. The Notice Letters sent to Plaintiffs and Class Members stated that Full Names and Social Security numbers were accessed and exfiltrated in the Data Breach.

55. As a result of the Data Breach, Plaintiffs and at least 51,659 Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

56. Defendant waited over 9 months to disclose the Data Brach to Plaintiffs and Class Members. As a result of this delay, Plaintiffs and Class Members had no idea their PII had been compromised in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

57. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

58. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members.

59. Despite recognizing its duty to do so, on information and belief, LDSC has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, LDSC leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

08936cb9558c.shtml (last visited January 4, 2024).

60. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII which includes information that is static, does not change, and can be used to commit myriad financial crimes.

61. Plaintiffs and Class Members relied on Defendant, as a third-party administrative company, to keep their PII confidential and securely maintained, to use their PII for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand Defendant safeguard their PII.

62. The unencrypted PII of Plaintiffs and Class Members will likely end up for sale on the Dark Web as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

63. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII.

The Data Breach Was Foreseeable

64. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting financial institutions that collect and store PII, like Defendant, preceding the date of the breach.

65. In light of recent high profile data breaches at other financial companies, Defendant knew or should have known that their electronic records and consumers' PII that it stored and maintained would be targeted by cybercriminals and ransomware attack groups.

66. In 2021, a record 1,862 data breaches occurred, resulting in approximately

293,927,708 sensitive records being exposed, a 68% increase from 2020.[11]

67. Because of the recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

68. Indeed, cyberattacks on financial-related companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, potential attack.[12]

69. Generally, "[c]ybercriminals choose their targets based on two conditions – maximum impact and maximum profit . . . [f]inancial institutions perfectly meet these conditions because they store highly valuable data, and their digital transformation efforts are creating greater opportunities for cyber attackers to access that data."[13]

Defendant Had an Obligation to Protect the PII

70. Defendant's failure to adequately secure Plaintiffs and Class Members' PII breaches duties it owes Plaintiffs and Class Members under statutory and common law. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under

---

[11] *See* 2021 Data Breach Annual Report, ITRC 6 (Jan. 2022), available at https://www.idtheftcenter.org/notified (last visited Jan. 12, 2024).

[12] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 12, 2024).

[13] Edward Kost, 10 Biggest Data Breach in Finance [Updated August 2022], UpGuard, (Ma. 2, 2023), https://www.upguard.com/blog/biggest-data-breaches-financial-services.

the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

71. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. S*ee, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

72. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

73. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiffs and Class Members.

74. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII in its possession was adequately secured and protected.

75. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained substandard data security systems.

76. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

77. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

78. Defendant owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

79. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

80. Defendant owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

81. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

82. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, at least, tens of thousands of individuals' PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Value of PII

83. The PII of individuals remains of high value to criminals, as evidenced by the prices criminals will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

84. Based on the foregoing, the information compromised in the Data Breach, including full names matched with Social Security numbers, is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

85. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[17]

---

[14] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 12, 2024).

[15] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan. 12, 2024).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 12, 2024).

[17] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 12, 2024).

86. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

87. The fraudulent activity resulting from the Data Breach may not come to light for years as there may be a time lag between when harm occurs versus when it is discovered, and also between when the PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

88. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

89. Plaintiffs and Class Members now face a lifetime of constant surveillance of their financial and personal records, credit monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

90. Defendant has acknowledged the risk and harm caused to Plaintiffs and Class Members as a result of the Data Breach. Defendant, to date, has offered Plaintiffs and Class Members abbreviated, non-automatic credit monitoring services. The limited credit monitoring is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come,

[18] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 12, 2024).

particularly in light of the PII at issue here. Moreover, Defendant put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services.

Defendant Failed to Properly Protect Plaintiffs' and Class Members' PII

91. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

92. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

93. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

94. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[19]

[19] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business,* FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last visited Jan. 12, 2024).

95. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for their respective lifetimes.

96. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent

programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[20]

97. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to

[20] *Id.* at 3-4.

verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[21]

98. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

[21] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Jan. 12, 2024).

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[22]

99. Moreover, given that Defendant was storing the PII of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

100. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiffs and Class Members.

101. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII.

102. Because Defendant failed to properly protect and safeguard Plaintiffs' and Class Members' PII, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files and exfiltrate that data.

[22] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020). https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Jan. 12, 2024).

Defendant Failed to Comply with Industry Standards

103. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

104. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

105. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

106. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

107. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

108. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards.

Defendant Fails to Comply with FTC Guidelines

109. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

110. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[23]

111. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[24]

112. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

[23] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

[24] *Id.*

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

113. The FTC has brought enforcement actions against financial institutions for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

114. These FTC enforcement actions include actions against financial institutions, like Defendant.

115. Defendant failed to properly implement basic data security practices.

116. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

117. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its clients' employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with the Gramm-Leach-Bliley Act

118. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

119. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding

Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

120. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

121. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

122. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

123. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security

and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

124. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendant's network systems.

125. Defendant failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

126. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing

and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

127. As alleged herein, Defendant violated the Safeguard Rule.

128. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

129. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendant's Negligent Acts and Breaches

130. Defendant participated in and controlled the process of gathering the PII from Plaintiffs and Class Members.

131. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiffs and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendant breached these obligations to Plaintiffs and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies for its health providers network that would adequately safeguarded Plaintiffs' and Class Members' PII. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiffs' and Class Members' PII;

b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c. Failing to test and assess the adequacy of its data security system;

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to put into develop and place uniform procedures and data security protections for its healthcare network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

h. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

i. Failing to implement or update antivirus and malware protection software in need of security updating;

j. Failing to require encryption or adequate encryption on its data systems;

k. Otherwise negligently and unlawfully failing to safeguard Plaintiffs' and Class Members' PII provided to Defendant, which in turn allowed cyberthieves to access its IT systems.

COMMON INJURIES & DAMAGES

132. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

133. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred

mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution or loss of value of their PII; and (h) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Risk of Identity Theft to Plaintiffs and Class Members Is Present and Ongoing

134. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

135. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

136. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

137. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[25] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[26] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

138. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[27] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[28] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[29]

139. Social Security numbers, for example, are among the worst kind of personal

[25]Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Jan. 12, 2024).

[26] *Id.*

[27] *What is the Dark Web?* – Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited Jan. 12, 2024).

[28] *Id.*; *see also* Louis DeNicola, *supra* note 25.

[29] *Id.*

information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[30]
>
> What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

140. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[31]

141. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social

[30] Social Security Administration, *Identity Theft and Your Social Security Number* (2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 12, 2024).

[31] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Jan. 12, 2024).

Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[32]

142. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[33]

143. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[34] Defendant did not rapidly report to Plaintiffs and Class Members that their PII had been stolen.

144. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

145. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

---

[32] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 12, 2024).

[33] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited Jan. 12, 2024).

[34] *Id.*

146. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

147. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[35]

148. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[36]

149. According to the FTC, unauthorized PII disclosures are extremely damaging to

[35] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), FTC (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Jan. 12, 2024).

[36] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Jan. 12, 2024).

consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[37]

150. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

151. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

152. Thus, due to Defendant's admitted recognition of the actual and imminent risk of identity theft, Defendant offered Plaintiffs and Class Members abbreviated, non-automatic credit monitoring services.

153. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting

[37] *See, e.g., Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last visited Jan. 12, 2024).

agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

154. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[38]

155. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

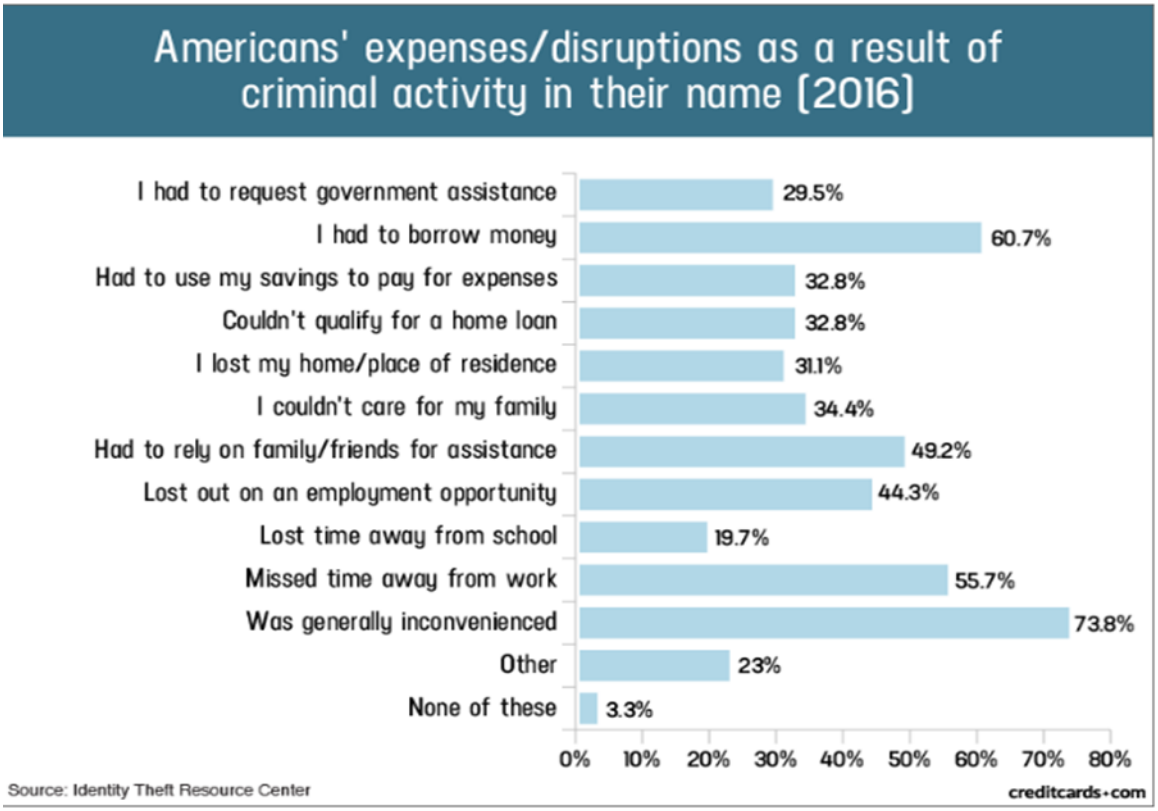
156. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[40]

---

[38] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 12, 2024).

[39] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Jan. 12, 2024).

[40] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://web.archive.org/web/20190304002224/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Jan. 12, 2024).



157. Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[41]

Diminution of Value of the PII

158. PII is a valuable property right.[42] Its value is axiomatic, considering the value of

[41] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Jan. 12, 2024).

[42] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4

Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

159. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

160. PII can sell for as much as $363 per record according to the Infosec Institute.[43]

161. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[44] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[45, 46] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[47]

162. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an

(2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[43] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 12, 2024).

[44] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers ((last visited Jan. 12, 2024).

[45] https://datacoup.com/.

[46] https://digi.me/what-is-digime/.

[47] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 12, 2024).

inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

163. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach.

164. The abbreviated, non-automatic credit monitoring offered to persons whose PII was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face ongoing identity theft and financial fraud for the remainder of their lives. Defendant also places the burden squarely on Plaintiffs and Class Members by requiring them to independently sign up for that service, as opposed to automatically enrolling all victims of this Data Breach.

165. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

166. It must be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

167. Such fraud may go undetected until debt collection calls commence months, or even

years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

168. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[48] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

169. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

170. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year, or more, per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Injunctive Relief Is Necessary to Protect against Future Data Breaches

171. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure

[48] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Jan. 12, 2024).

that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

Plaintiffs' Individual Experiences

Plaintiff Shira Kohn's Experience

172. Plaintiff Kohn received the Notice Letter, by U.S. mail, directly from Defendant, dated August 4, 2023. According to the Notice Letter, Plaintiff Kohn' PII was improperly accessed and obtained by unauthorized third parties, including her name and Social Security number.

173. Plaintiffs' Notice Letter stated that Defendant provides certain retirement planning services for the Savannah College of Art and Design.

174. Plaintiff was a student from 2012 to 2016 and an employed as a Student Ambassador from 2013 to 2016 at the Savannah College of Art and Design, however Plaintiff Kohn did not participate, and has never participated in a retirement plan with the Savannah College of Art and Design.

175. As a condition of her employment, Plaintiff Vivas was required to provide her PII, indirectly or directly, to Defendant.

176. At the time of the Data Breach—on or about October 18, 2022—Defendant retained Plaintiff Kohn's PII in its system, despite Plaintiff Kohn no longer being employed at Defendant's client for approximately six years.

177. As a result of the Data Breach, Plaintiff Kohn spent time dealing with the consequences of the Data Breach, which includes placing a security freeze on her credit reports, verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and/or credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Notice

Letter where Defendant advised Plaintiff Kohn to mitigate her damages by, among other things, freezing her credit reports and monitoring her accounts for fraudulent activity.

178. Additionally, Plaintiff Kohn suffered actual injury when she was notified by her Equifax credit monitoring services that her Social Security number was found on a fraudulent internet trading site on the Dark Web on August 17, 2023, which upon information and belief, was caused by the Data Breach.

179. Plaintiff Kohn is a cautious person and is therefore very careful about sharing her sensitive PII. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Kohn stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Kohn diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be.

180. The Data Breach caused Plaintiff Kohn to suffer a loss of privacy.

181. Plaintiff Kohn has also experienced an increase in the number of spam calls and emails since the Data Breach.

182. The Data Breach has caused Plaintiff Kohn to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

183. As a result of the actual harm she has already suffered, and the substantial present risk of additional harm that he will face the rest of her life, Plaintiff Kohn spent valuable time freezing her credit reports with all three major credit bureaus.

184. The loss of privacy and substantial present risk of additional imminent harm have both caused Plaintiff Kohn to suffer stress, fear, and anxiety as Plaintiff Kohn is very concerned

that her sensitive PII is now in the hands of data thieves and shall remain that way for the remainder of her lifetime and there is nothing Plaintiff Kohn can do to retrieve her stolen PII from the cyber-criminals.

185. Plaintiff Kohn is aware of no other source from which the theft of her PII could have come. She regularly takes steps to safeguard her own PII in her own control.

186. Given the time Plaintiff Kohn has lost investigating this data breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Kohn's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Kohn's valuable PII, the damages articulated more specifically above are far from the full extent of the harm thereto.

Plaintiff Andres Vivas' Experience

187. Plaintiff Andres Vivas is a former employee of The Savannah College of Art and Design, working there from approximately 2013 to 2015.

188. Upon information and belief, The Savannah College of Art and Design contracted with Defendant for services.

189. As a condition of receiving Defendant's services, Plaintiff Vivas was required to provide his PII, indirectly or directly, to Defendant.

190. At the time of the Data Breach—on or about October 18, 2022—Defendant retained Plaintiff Vivas' PII in its system, despite Plaintiff Vivas no longer being employed at Defendant's client for approximately seven years.

191. Plaintiff Vivas is very careful about sharing his sensitive PII. Plaintiff Vivas stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Vivas would

not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

192. Plaintiff Vivas received the Notice Letter, by U.S. mail, directly from Defendant, dated August 4, 2023. According to the Notice Letter, Plaintiff Vivas' PII was improperly accessed and obtained by unauthorized third parties, including his name and Social Security number.

193. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Vivas made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, contacting credit bureaus to ensure his accounts are secured, and checking his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff Vivas otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

194. Plaintiff Vivas suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

195. Additionally, Plaintiff Vivas suffered actual injury in the form of experiencing identity theft in the form of a fraudulent Home Depot credit card application being submitted

falsely under his name, in or about September 2023, which upon information and belief, was caused by the Data Breach.

196. Plaintiff further suffered actual injury in the form of experiencing identity theft in the form of a fraudulent Kohl's credit card application being submitted falsely under his name, in or about September 2023, which upon information and belief, was caused by the Data Breach.

197. Plaintiff Vivas further suffered actual injury in the form of his PII being disseminated on the dark web, according to Experian, which upon information and belief, was caused by the Data Breach.

198. Plaintiff Vivas further suffered actual injury in the form of his credit score being damaged as a result of the fraudulent hard inquiries on his account, which upon information and belief, was caused by the Data Breach.

199. Plaintiff Vivas also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which upon information and belief, was caused by the Data Breach.

200. The Data Breach has caused Plaintiff Vivas to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

201. As a result of the Data Breach, Plaintiff Vivas anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

202. As a result of the Data Breach, Plaintiff Vivas is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

203. Plaintiff Andres Vivas has a continuing interest in ensuring that his PII, which, upon

information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

204. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

205. The nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII was compromised in the Data Breach event including all individuals who received the Notice of Security Event that Defendant published to Plaintiffs and other Class Members beginning on or around August 4, 2023 (the "Class").

206. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

207. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

208. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there at least multiple thousands of individuals who were notified by Defendant of the Data Breach. According to the report submitted to the Maine Attorney's General office, 51,659 individuals had their PII compromised in this Data

Breach.[49] The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

209. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in

[49] See Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/f7119163-666d-4163-8805-08936cb9558c.shtml (last visited Jan. 12, 2024).

the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

210. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

211. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

212. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent

and protect the interests of the Class Members in that Plaintiffs has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously.

213. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

214. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that

experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

215. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

216. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

217. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

218. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

219. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Putative Rule 23 Class)

220. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 221.

221. Defendant requires its clients' employees, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of providing its services.

222. Defendant gathered and stored the PII of Plaintiffs and Class Members as part of its business of soliciting its services to its clients and its clients' employees, which solicitations and services affect commerce.

223. Plaintiffs and Class Members entrusted Defendant with their PII, directly or indirectly, with the understanding that Defendant would safeguard their information.

224. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

225. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

226. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

227. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

228. Defendant owed a duty of care to Plaintiffs and Class Members to provide data

security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

229. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its clients' employees. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary part of being employees of Defendant's clients.

230. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

231. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

232. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

233. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

234. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

235. Defendant breached its duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect

Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

236. Defendant violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

237. Plaintiffs and Class Members were within the class of persons the Federal Trade

Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

238. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes negligence.

239. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

240. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

241. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

242. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

243. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

244. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

245. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly

remains in, Defendant's possession.

246. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

247. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

248. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

249. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

250. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

251. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach; (vii) Plaintiff Vivas experiencing identity theft in the form of an attempt to open a Home Depot credit card falsely under his name in September 2023; (viii) Plaintiff Vivas experiencing identity theft in the form of an attempt to open a Kohl's credit card falsely under his name in September 2023; (ix) Plaintiff Vivas' credit score being damaged, as a result of recent fraudulent hard inquiries on his account; (x) Plaintiff Vivas' PII being disseminated on the dark web, according to Experian; (xii) Plaintiff Kohn's Social Security number be disseminated on the dark web, according to Equifax; (xi) an increase in spam calls, texts, and/or emails; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

252. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

253. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

254. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

255. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs

and Class Members in an unsafe and insecure manner.

256. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiffs and the Putative Rule 23 Class)

257. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 221.

258. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

259. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

260. Defendant owed a duty of care in protecting Plaintiffs' and Class Members' PII, pursuant to Section 5 of the FTC Act, GLBA, and an independent duty of care.

261. Defendant violated Section 5 of the FTC Act, GLBA, and similar state statutes by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

262. In its Privacy Policy, Defendant promises its clients' employees that it will not disclose their PII, outside of the excepted circumstances set forth therein—none of which apply here. However, Plaintiffs' and Class Members' PII has been disclosed without their written authorization as a result of the Data Breach.

263. As evidenced by the occurrence of the Data Breach, Defendant negligently misrepresented its data security measures and Privacy Policy to Plaintiffs and Class Members.

264. Defendant violated Section 5 of the FTC Act and GLBA by negligently misrepresenting its data security practices to Plaintiffs and Class Members.

265. Defendant violated Section 5 of the FTC Act and GLBA by breaching its duties of care to Plaintiffs and Class Members, as provided in its Privacy Policy.

266. Defendant further violated Section 5 of the FTC Act and GLBA by failing to ensure that its vendors use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and shared and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

267. Defendant's violation of Section 5 of the FTC Act, GLBA, and other duties (listed above) constitutes negligence *per se.*

268. Class members are customers within the class of persons that Section 5 of the FTC Act, GLBA, and similar state statutes intended to protect.

269. Moreover, the harm that has occurred is the type of harm that the FTC Act, GLBA, and similar state statutes were intended to guard against. Indeed, the FTC has pursued over numerous enforcement actions against insurance companies which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices,

caused the same harm suffered by Plaintiffs and Class Members.

270. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

271. There is a close causal connection between Defendant's failure to implement or ensure security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

272. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) Plaintiff Vivas experiencing identity theft in the form of an attempt to open a Home Depot credit card falsely under his name in September 2023; (viii) Plaintiff Vivas experiencing identity theft in the form of an attempt to open a Kohl's credit card falsely under his name in September 2023; (ix) Plaintiff Vivas' credit score being damaged, as a result of recent fraudulent hard inquiries on his account; (x) Plaintiff Vivas' PII being disseminated on the dark web, according to Experian; (xii) Plaintiff Kohn's Social Security number be disseminated on the dark web, according to Equifax; (xi) an increase in spam calls, texts, and/or emails; and (xii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b)

remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

273. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

274. As a direct and proximate result of Defendant's negligence *per se*, the products and/or services that Defendant provided to Plaintiffs and Class Members damaged other property, including the value of their PII.

275. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

276. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

277. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

278. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Breach Of Third-Party Beneficiary Contract
(On behalf of Plaintiffs and the Putative Rule 23 Class)

279. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 221.

280. Upon information and belief, Defendant entered into virtually identical contracts with its clients, including Plaintiffs' and Class Members' former employers, to provide services to its clients, which included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be entrusted to it.

281. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their PII that Defendant agreed to receive and protect through their services. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

282. Defendant knew that if they were to breach these contracts with their clients, Plaintiffs and the Class, would be harmed.

283. Defendant breached their contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

284. As foreseen, Plaintiffs and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in their care, including but not limited to, the continuous and substantial risk of harm through the loss of their PII.

285. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiffs and the Putative Rule 23 Class)

286. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 221. Notwithstanding, Plaintiffs bring this claim in the alternative to any claim for breach of contractual obligations.

287. Defendant benefited from receiving Plaintiffs' and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

288. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

289. Defendant was also enriched from the value of Plaintiffs' and Class Members' PII. PII has independent value as a form of intangible property. Defendant also derives value from this information because it allows Defendant to operate its business and generate revenue.

290. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

291. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

292. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

293. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

294. Plaintiffs and Class Members have no adequate remedy at law.

295. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

296. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

297. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Putative Rule 23 Class)

298. Plaintiffs re-allege and incorporate by reference herein all of the allegations

contained in paragraphs 1 through 221.

299. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' PII; (2) to timely notify Plaintiffs and Class Members of the Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

300. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with its customers, in particular, to keep secure their PII.

301. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

302. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' PII.

303. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

304. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII.

305. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii)

out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

306. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiffs and their Counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive

and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: January 12, 2024

Respectfully Submitted,

s/ Justin C. Walker

Justin C. Walker (admitted *pro hac vice*)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
jwalker@msdlegal.com

Interim Class Counsel for Plaintiffs and Putative Rule 23 Class

John J. Nelson (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Interim Class Counsel for Plaintiffs and Putative Rule 23 Class

Joe Kendall
Texas Bar No. 30973
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Phone:214-744-3000
Fax: 214-744-3015
jkendall@kendalllawgroup.com

Interim Texas Local Counsel for Plaintiffs and Putative Rule 23 Class

Terence R. Coates (admitted *pro hac vice*)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Gary M. Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
glkinger@milberg.com

Counsel for Plaintiffs and Putative Rule 23 Class

CERTIFICATE OF SERVICE

I hereby certify that on this 12th day of January 2024, I caused a true and correct copy of the foregoing to be filed with the Clerk of the Court for the Southern District of Texas via the Court's CM/ECF system, which will send notification of such filing to the counsel of record in the above-captioned matters.

/s/ Justin C. Walker
Justin C. Walker